

DOCKET FILE COPY ORIGINAL

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of

Policies and Rules Concerning  
Toll Fraud

)  
)  
)  
)

CC Docket No. 93-292

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

COMMENTS OF GTE

GTE Service Corporation and its affiliated  
domestic telephone, equipment and service  
companies

David J. Gudino  
1850 M Street, N.W.  
Suite 1200  
Washington, DC 20036  
(202) 463-5212

January 14, 1994

Their Attorney

No. of Copies rec'd  
List ABCDE

014

## TABLE OF CONTENTS

	<u>PAGE</u>
SUMMARY .....	iii
DISCUSSION .....	1
I. INTRODUCTION .....	1
II. THE FOCUS OF ALL ACTIVITY, INCLUDING THE COMMISSION'S, SHOULD BE ON FRAUD PREVENTION, NOT ON ASSIGNMENT OF LIABILITY.....	2
III. SUCCESSFUL TOLL FRAUD PREVENTION AND DETECTION REQUIRES A COOPERATIVE EFFORT ON THE PART OF ALL TELECOMMUNICATIONS USERS, EQUIPMENT VENDORS, AND NETWORK SERVICE PROVIDERS.....	4
A. PBX FRAUD .....	4
B. PAYPHONE FRAUD .....	6
C. CELLULAR FRAUD.....	13
D. LINE INFORMATION DATABASE FRAUD (LIDB).....	15
1. Calling Card Fraud .....	16
2. Provision of the Originating Calling Party Number and the Called Number .....	19
3. Tariff Limitations of Liability v. Allocation of Liability.....	21
E. OTHER PROPOSALS AND REQUESTS FOR COMMENT .....	23
1. Effect of Billing and Collection Agreements on Toll Fraud Prevention Incentives .....	23
2. The Effect of Network Changes on Toll Fraud Prevention and Detection .....	24
3. Carrier Release of Network Change Information .....	26

IV. THERE ARE ACTIONS THE COMMISSION CAN TAKE TO ASSIST IN COMBATING TOLL FRAUD .....	28
A. PAYPHONE ACTIVITIES .....	28
B. CUSTOMER INFORMATION ACTIVITIES .....	29
C. ACTION TO ENCOURAGE COOPERATION AMONG SERVICE PROVIDERS .....	29
D. ENFORCEMENT LEGISLATION .....	30

## **SUMMARY**

It is the inherent responsibility of all parties involved in providing and using telecommunication equipment and/or services to take all reasonable measures to prevent toll fraud. This includes education of users and installation of prevention measures and detection systems. Toll fraud must be addressed at the most cost-effective location, whether in CPE or in the network, whichever provides the greatest capability for the least cost. Equally important is the proper use of these fraud prevention/detection tools. Any arbitrary allocation of liability will only skew the incentives necessary for global participation in this effort. Consequently, the Commission should focus its efforts on promoting education, deterrence, and prosecution.

Exchange carriers have limited ability to prevent PBX-based toll fraud. Monitoring capabilities inherent in a PBX are the most efficient way to address this form of toll fraud. Any new exchange carrier monitoring offerings required by the Commission should be created only when it is economically viable.

GTE is eager to work with its payphone CPE customers not only in the selection of equipment, but in providing information on fraud prevention, assisting in detecting perpetrators, and resolving liability issues when fraud does occur. GTE acknowledges its responsibility for the accurate functioning of its blocking and screening services. However, LECs cannot stop toll fraud; they can only assist in its prevention. Even with blocking and screening services, some amount of payphone toll fraud will occur due to a lack of proper use by payphone providers and Alternate Operator Services providers. Accordingly, private payphone providers must accept some degree of fraud liability just as other industry participants must.

Adequate cellular fraud prevention incentives exist for cellular service providers. The numerous efforts undertaken by GTE as well as other providers underscores this

fact. However, new legislation designed to specifically combat fraud is much needed to provide "bite" to this already aggressive segment of the industry.

GTE and other LIDB owners, as well as LIDB customers, already are actively engaged in calling card fraud prevention and detection. The Commission does not need to add "artificial" incentives for exchange carriers to continue in their fight against toll fraud. "Natural" incentives are already in place for exchange carriers. The effectiveness of LEC efforts is highly dependent upon cooperation between end user customers and other network service providers. Any exchange carrier that has reasonable fraud prevention measures in place and operating properly should not be arbitrarily allocated a share of interLATA or international toll fraud liability.

GTE's billing and collection agreements provide both direct and indirect incentives for toll fraud prevention and detection. One promising network-based prevention tool currently being evaluated by the industry is Originating Line Number Screening. Existing customer-service provider relationships, industry forums, and Commission rules are more than adequate to inform all interested parties of network changes that could influence toll fraud detection or prevention.

It is not necessary for the Commission to attempt to reinforce the incentives for toll fraud prevention and detection that already exist. Rather, the Commission can assist the telecommunications industry by: (i) encouraging organizations representing the interests of private payphone providers to educate their members on fraud prevention techniques; (ii) leading an effort to relax state and federal restrictions on the sharing of customer information needed to identify and combat toll fraud; (iii) require all entities subject to its jurisdiction to cooperate with a new agency that should be created to coordinate detection and prevention efforts; and (iv) encouraging a Congressional effort to create legislation that would clearly define and penalize toll fraud and give law enforcement agencies the tools needed to track and prosecute perpetrators of toll fraud.

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of

Policies and Rules Concerning  
Toll Fraud)  
)  
)  
)

CC Docket No. 93-292

**COMMENTS OF GTE**

GTE Service Corporation ("GTE"), on behalf of its affiliated domestic telephone, equipment, and service companies, offers its Comments to the Commission's Notice of Proposed Rulemaking ("*NPRM*") released December 2, 1993, FCC No. 93-496.

The *NPRM* addresses the issue of toll fraud in the telecommunications industry. In general, the Commission seeks comment on its proposals to: (1) achieve closer coordination between the industry, consumers, vendors, law enforcement, Congress and the Commission to aid in the detection and prevention of toll fraud; (2) improve consumer education initiatives by the Commission, consumer groups and the telecommunications industry; (3) determine that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of toll fraud risks of using carrier services are unreasonable; (4) establish a federal policy assigning liability for payphone fraud; (5) codify a requirement for written warnings for all telecommunications equipment registered under Part 68; and, (6) determine measures to prevent cellular and Line Information Database ("LIDB") fraud.

**DISCUSSION****I. INTRODUCTION**

No one can dispute that toll fraud has long been a problem in the telecommunications industry. Experience has shown that virtually every advance in

telecommunications has been paralleled by a correlating advance in "hacking" techniques. Toll fraud currently drains billions of dollars in revenues from the industry on an annual basis; revenues that, in most instances, are never recovered. And as the Commission notes, "[c]ontrol over the use of telecommunications services has increasingly shifted from carriers to individual consumers." (*NPRM* at ¶ 3.) With this shift, a whole new class of targets has emerged. "Customers, as well as carriers, are now the victims." (*Id.*)

GTE fully endorses the Commission's effort to address this problem on a global basis. In the past, attempts to deter and prosecute toll fraud have been largely isolated efforts. More recently, however, numerous voluntary joint efforts aimed at combating toll fraud have surfaced. As discussed below, detection techniques and prevention methods are being developed and deployed on a widespread basis. But in order for the effort to be most effective, all players, from carriers to manufacturers to alternative services providers to law enforcement to the final user must be actively involved. Any heavy-handed rule-making aimed at allocating liability "once and for all" will only undermine this effort by skewing existing incentives to combat fraud.

**II. THE FOCUS OF ALL ACTIVITY, INCLUDING THE COMMISSION'S, SHOULD BE ON FRAUD PREVENTION, NOT ON ASSIGNMENT OF LIABILITY.**

Everyone involved in using or providing telecommunications equipment or services must have an incentive to fulfill its unique role. In this context, arbitrarily placing liability on certain persons or entities is like placing a Band-Aid on a cancerous mole. The mole can no longer be seen but the cancer continues because a Band-Aid is not effective treatment. In the same way, hard and fast liability rules may please those falling outside the liability umbrella and so "solve" the problem for them, but they will not "treat" the underlying problem of toll fraud. To the contrary, they only will make toll fraud worse by promoting apathy among those whose involvement is critically

needed but who find themselves suddenly unaffected by it and so less inclined to get involved.

Unfortunately, in this context where crime is involved, potential monetary loss appears to be the only truly universal incentive for effective global participation.<sup>1</sup> Such participation is needed because new detection and prevention techniques must be developed *and* used properly; information on new forms of toll fraud must be disseminated quickly to potential victims; more secure products and services must be developed; and full cooperation in prosecuting hackers must become a given.

Like the traveling con man, hackers are most successful when they are not anticipated. Known forms of hacking remain effective because they are continually being used on new groups of victims unaware of how they work. A global effort at battling toll fraud will result in an industry that, down to the end-user, will *anticipate* rather than *react* to fraud. As discussed below, the industry has already taken major steps in this direction. Thus, GTE urges the Commission to focus its efforts and those of everyone involved in providing or using telecommunications equipment or services on promoting education, deterrence, and prosecution rather than on dealing with the aftermath of the problem through the allocation of liability.

*In summary:* The battle against toll fraud will require a concerted effort by everyone involved in providing or using telecommunications equipment or services. Any arbitrary allocation of liability will only skew the incentives necessary for global

---

<sup>1</sup> Local Exchange Carriers ("LECs" or "exchange carriers") already have every incentive to take every reasonable measure to prevent toll fraud. Even in those instances where a LEC is not liable for the fraud, it still has incentives to prevent its reoccurrence. Fraudulent toll charges often result in costly collection efforts as customers either refuse to pay or initiate legal action of their own. Moreover, in the age of increased competition, it is bad business for a LEC to be engaged in such conflicts with its own customers.

participation in this effort. Consequently, the Commission should focus its efforts on promoting education, deterrence, and prosecution.

**III. SUCCESSFUL TOLL FRAUD PREVENTION AND DETECTION REQUIRES A COOPERATIVE EFFORT ON THE PART OF ALL TELECOMMUNICATIONS USERS, EQUIPMENT VENDORS, AND NETWORK SERVICE PROVIDERS.**

In the *NPRM*, the Commission discusses various types of toll fraud, sets forth several tentative conclusions, and asks for comment on a number of issues. These Comments are organized in a similar manner. Each section describes prevention and/or detection techniques for each form of toll fraud, and provides specifics on GTE's activities.

**A. PBX FRAUD.**

The Commission seeks comment on "whether to require IXCs and LECs to offer customers protection through monitoring services, [and] on what basis those services should be offered."<sup>2</sup> (*NPRM* at ¶ 26.) Monitoring call activity on PBXs through the use of exchange carrier network capability is far less efficient than using PBX-based monitoring techniques. Modern PBXs have virtually all of the sophisticated capabilities found in exchange carrier end office switches. These include call detail recordings that allow the PBX owner to examine a listing of all toll calls for each station or account

---

<sup>2</sup> GTE does not manufacture PBX equipment; it acts only as a sales agent for equipment manufactured by others. Thus, GTE will not engage in an expansive discussion of PBX toll fraud issues, but rather recommends that the Commission review a position paper entitled "A Cooperative Solution to the Fraud that Targets Telecom Systems" prepared by the Toll Fraud Prevention Committee ("TFPC") of the Alliance for Telecommunications Industry Solutions ("ATIS"). This paper exhaustively describes the actions that can be taken by equipment vendors, end users, communications consultants, sales personnel, network services providers, regulators, law enforcement agencies, and legislators to combat PBX fraud. GTE participates in TFPC activities and endorses the views expressed in its paper.

number, restrictions on certain types of incoming or outgoing calls by station or account number, and thresholds for monitoring purposes. Older PBXs can be retrofitted with outboard devices that provide much of this same functionality.<sup>3</sup>

The role of the exchange carrier in minimizing PBX toll fraud is limited largely to providing its PBX customer with the information necessary to allow the customer to fully understand the capabilities of the equipment. The exchange carrier also can provide fraud prevention tips and periodic reminders of the need for diligence through billing inserts and direct customer contact.<sup>4</sup>

All toll fraud prevention and detection measures should be accomplished in the most cost effective manner possible. In the context of the PBX, simply adding capabilities to the exchange carrier network is neither the best nor the most efficient way to combat PBX fraud. However, should the Commission require exchange carriers to create new service offerings, the guiding principle should be based on the feasibility criteria found useful in creating unbundled Open Network Architecture offerings; *i.e.*, customer utility, technical feasibility, adequate market demand, and costing feasibility.<sup>5</sup> Using this criteria, exchange carriers would only be required to develop and offer toll fraud monitoring services when it becomes economically viable to do so.<sup>6</sup>

---

<sup>3</sup> See *NPRM* at ¶ 41 (discussion of the equipment offered by Science Dynamics Corporation).

<sup>4</sup> Attachment A contains examples of the literature GTE provides to its PBX customers describing typical methods used to perpetrate PBX toll fraud and actions that can be taken to prevent losses.

<sup>5</sup> *Filing and Review of Open Network Architecture Plans*, 4 FCC Rcd 1, 207 (1988).

<sup>6</sup> The existence of incentives will play a critical role in establishing economic viability. That is, services will be offered only when a demand for them develops. However, a demand will develop only if PBX customers have an incentive to purchase the services. In turn, they only will have an incentive to purchase if potential exposure from fraud is a part of their cost of doing business.

*In summary.* Exchange carriers have limited ability to prevent PBX-based toll fraud. The most efficient way to address this form of toll fraud is through the monitoring capabilities inherent in a PBX. Any new exchange carrier monitoring offerings required by the Commission should be created only when it becomes economically viable to do so.

#### **B. PAYPHONE FRAUD.**

Referencing the Florida Public Service Commission ("FPSC") proceeding,<sup>7</sup> the Commission notes that, "many commenters contend that the emphasis for any fraud proposal should be on fraud prevention, not on the apportionment or assignment of liability."<sup>8</sup> GTE agrees with this reasoning and believes that if proper prevention and detection techniques are deployed *and* used properly, toll fraud will be reduced to such a degree that assignment of liability will no longer be a significant issue. It is important for the Commission and all parties affected by toll fraud to recognize that toll fraud will never cease to exist. Even with the most sophisticated techniques possible, there will still be individuals capable of circumventing detection. But, with a cooperative effort of all industry segments and affected end users, toll fraud can be detected and prevented to a much greater degree. In light of these realities, it is counterproductive and indefensible to impose sole liability for toll fraud only on certain segments of the telecommunications industry such as the LECs or Interexchange Carriers ("IXCs").

In analyzing payphone toll fraud, measures that all payphone providers, including LECs, IXCs, and private payphone providers, can take to prevent toll fraud

---

<sup>7</sup> Florida Public Service Commission Petition for Review of Interstate and International Tariff Provisions Relating to Liability for Toll Fraud Charges, File No. 93-TOLL FRAUD-02, filed February 18, 1993. ("FPSC Petition.")

<sup>8</sup> *NPRM* at ¶ 30.

must be considered. For most LEC-owned and operated coin phones, special end office circuitry is provided (e.g., coin terminating line cards, special power supplies, and outgoing trunks equipped to handle coin lines) in addition to special software database translations. LEC Operator Services Systems ("OSSs"), either automated or operator handled, have mechanisms to assist in the prevention of toll fraud. Automated OSSs are programmed to accurately record and verify the validity of billing information on originating and terminating calls and LEC operators receive intensive and continuing training on proper call recording and handling. This includes checking the called number on collect calls to determine if it is a payphone, securing proper acceptance of charges on collect calls, verification that bill-to-third number calls are not being billed to a payphone or a number that does not allow such billing, securing calling card validation, and the collection of the correct amount on coin sent-paid calls. LECs update the LIDB on a regular basis with LEC payphone numbers so that an operator can verify whether or not the billed number is a payphone.

Private payphone providers also have a responsibility to utilize all reasonable preventative measures to limit payphone toll fraud. One of these measures is the selection of an Alternate Operator Services ("AOS") provider that performs operator services functions necessary to ensure that billing information is accurately recorded and verified. Should the Commission take any action regarding payphone fraud, it should require that all AOS providers subscribe to LEC screening and/or blocking services, and provide their operators with comprehensive training and operating procedures that ensure they perform the required checks. LECs should not be responsible for payphone toll fraud resulting from an AOS provider not accurately recording or verifying billing information.

The proper selection of Customer Premises Equipment ("CPE") by private payphone providers also can help mitigate fraud. Private payphone CPE ranges from the very simple to the extremely sophisticated. Programmable payphones can provide

originating call blocking along with special "cuckoo" tones to prevent incoming collect calls. Adjunct devices also are available that can be used to prevent fraud on less sophisticated CPE. Another very important fraud prevention technique is the selection of well lighted and observable locations for payphones where suspicious activities can be more readily detected. All of these measures are under the sole control of the private payphone provider. Consequently, these providers must recognize their obligation to know the limitations of their CPE and to take appropriate fraud preventative measures such as the addition of adjunct devices, verification of proper programming, replacement of obsolete equipment, etc. GTE works closely with its CPE customers in the battle against fraud by explaining CPE capabilities, toll fraud techniques, and available prevention and detection measures. But, it is the payphone owner that ultimately decides which CPE to purchase and how it will be programmed and protected.

Other fraud prevention measures available to private payphone providers include LEC screening and blocking services. LECs have developed services such as Billed Number Screening ("BNS") that provides for the automatic blocking of incoming bill-to-third number calls, collect calls, or both. GTE has tariffed BNS in the majority of the states it serves and is proceeding actively to tariff it in those remaining. GTE's rates per screened individual access line range from free to \$5 a month, depending upon prevailing state regulations. BNS also is offered on a lower cost bulk basis for customers with 50 or more lines. GTE's records indicate that approximately 90 percent of private payphone providers subscribe to BNS.<sup>9</sup>

---

<sup>9</sup> This percentage is based upon lines that GTE knows to be private payphone lines. Not all private payphone lines are recognizable by GTE since not all private payphone providers inform GTE that the line will be used for a payphone.

GTE offers other options such as Selective Class of Call Screening ("SCCS"). This service provides customers with a choice of originating call screening options whenever an operator service system is involved with call processing. SCCS options are offered on either a line or trunk basis and include: (1) bill to a calling card account; (2) bill-to-third number; (3) collect to the called number; or (4) prohibit all operator assisted sent-paid calls. These types of calls are flagged so that the operator is aware that special call handling is required. The operator performs a database check and receives instructions on whether the call can be completed as dialed. SCCS is offered in most of GTE's state tariffs and, like BNS, GTE anticipates offering this service in all of its operating areas. The rates for SCCS individual access line screening range from free to \$6 per month, depending upon prevailing state regulations.<sup>10</sup> GTE's records indicate that approximately 90 percent of private payphone providers subscribe to some form of SCCS.<sup>11</sup>

GTE also offers blocking services for 900 and 976 originated calls in all of its state tariffs at no charge to the subscriber. Other GTE blocking options available in state tariffs involve toll restriction. One option restricts direct dialed 1+ or direct dialed international 011+ calls except for calls to 800 service which are not restricted. Another option includes the above option and restricts any local or long distance 0+ or 0- calls. If 911 service is not available in an exchange, 0- calls are restricted to operator assisted local calls and calls to governmental agencies. GTE also offers a service involving split blocking. This service blocks direct dialed domestic casual usage (10XXX+1+) and direct dialed international casual usage (10XXX+011+) calls that access an IXC other than the primary interexchange carrier selected for the line. GTE's

---

<sup>10</sup> Currently one state has a rate higher than \$6. GTE plans on filing tariffs seeking to lower this rate by the end of January 1994.

<sup>11</sup> Based upon private payphone lines GTE is able to recognize.

records indicate that the payphone provider subscription rate for 900/976 blocking is 66 percent and for 1+ blocking options three percent.<sup>12</sup>

International fraud consists of two types of calls: outbound and inbound.<sup>13</sup> Payphone providers with programmable CPE can perform outbound international call blocking at the payphone or can subscribe to LEC blocking services or use both methods to doubly insure against outbound international calls being placed. However, inbound international calling is a completely different situation. Inbound international fraud is a significant problem. It is extremely difficult to prevent not only for payphone providers, but also for the IXC's. Some private payphone providers want the IXC's to ensure that foreign operators perform screening and blocking checks by refusing to settle with the foreign carrier if the checks are not performed. But inbound international is controlled by the foreign operator, not the U.S. based IXC's, and any ruling by this Commission would not apply to foreign carriers or their operators. International accounting agreements are extremely difficult to negotiate. Adding required performance standards for foreign operators would make these negotiations impossible. In particular, attempting to force foreign operators to access a U.S. owned and operated database for which there would be accompanying charges would be an unrealistic expectation. Consequently, the IXC's and/or LEC's should not be held responsible for foreign operators' actions or be required to dictate to foreign entities what their operator practices should be. The simplest and most effective solution is for the private payphone provider to use CPE that has a "cuckoo" tone to inform operators that incoming collect calls are not allowed.

---

<sup>12</sup> Again, based upon private payphone lines GTE is able to recognize.

<sup>13</sup> Outbound international blocking is offered in General Telephone Operating Companies ("GTOC") Tariff FCC No. 1 at a rate of \$19.95 per month. Half of all private payphone providers known to GTE subscribe to this service.

LEC blocking and screening services are only tools to aid in the prevention of toll fraud. For these tools to be effective, however, they must be used and used properly. Thus, each party must assume responsibility for using those tools at its disposal. The payphone provider must subscribe to the services that meet its individual situation. In addition, the payphone provider must provide accurate and complete data to the LEC so that LEC databases performing blocking and screening functions operate to their fullest potential. The LEC must accurately record the information provided by the payphone provider, provision the blocking and screening services, and ensure that they are functioning properly. The operator services provider or the IXC must acknowledge the screening and/or blocking options and process calls accordingly. Although these tools are not the ultimate solution to toll fraud, they can be a powerful aid in its prevention when used as designed.

The Commission asks "whether the Florida approach has been an effective way of dealing with payphone fraud." (*NPRM* at ¶ 31.) While supporting the efforts of the FPSC in its attempt to reduce fraud, GTE does not believe that a nationwide policy or federal tariffing of blocking and screening services will serve to accomplish this goal. GTE's experience in Florida indicates that the FPSC's policy has been effective only in reducing the number of complaints filed by private payphone providers regarding fraud — the amount of fraud has not decreased.<sup>14</sup> The only change that has occurred is the assignment of liability. The private payphone providers have seen a reduction in fraudulent charges only because the LECs and IXCs must now assume this liability.

The Florida experience shows that any policy that merely reassigns liability for fraud will only mask its presence, not prevent it. If private payphone providers are

---

<sup>14</sup> GTE only can speculate that: AOS providers are not performing verification; CPE malfunctions are occurring; and/or incorrect data has been provided to LECs for input into their databases.

relieved of any responsibility for fraud simply by purchasing LEC blocking and screening options, they will no longer have the incentive to take all other available precautions that are vital to the effective prevention of toll fraud. The FPSC approach does not address preventative measures that private payphone providers should or must take other than LEC blocking and screening services. Further, liability is "allocated between the LECs and IXC's based on fault." (*NPRM* at ¶ 27.) But "fault" is difficult, if not impossible, to determine in many cases and should not be limited to LECs and IXC's only. Blocking and screening services are effective fraud prevention measures but they are not foolproof. Any Commission proposal addressing fraud prevention and/or liability issues should define the responsibilities of all participants; *i.e.*, LECs, IXC's, private payphone providers, and AOS providers. These responsibilities must include the use of all reasonable preventative measures available. The Commission would be ill-advised to adopt any policy that ignored vital participants in fraud prevention. Instituting such a policy at a national level would only exacerbate an already difficult situation.

The prices for LEC blocking and screening services should not pose a barrier to their use. But, if LECs are required to insure private payphone providers against toll fraud, then these rates must be increased to include the assumption of this liability. Compensatory rates for these services would have to be developed incorporating the liability being assumed by the LECs. The contention by some commenters that LECs and IXC's should absorb the costs of toll fraud because they "are much better able to absorb the costs of fraud than payphone providers"<sup>15</sup> should be wholly disregarded by the Commission. The financial status of a company should have no bearing on its liability.

---

<sup>15</sup> *NPRM* at ¶ 29.

*In summary:* GTE is eager to work with its payphone customers not only in the selection of CPE, but in providing information on fraud prevention, detecting perpetrators, and resolving liability issues when fraud does occur. GTE acknowledges its responsibility for the accurate functioning of its blocking and screening services. However, there is no way that any LEC can stop toll fraud; it can only assist in its prevention. Even with blocking and screening services, some amount of payphone toll fraud will occur. Accordingly, private payphone providers must accept some degree of fraud liability as the cost of doing business just as other industry participants must.

### **C. CELLULAR FRAUD.**

GTE believes that adequate cellular fraud prevention incentives exist for cellular service providers. Through the Cellular Telecommunications Industry Association's ("CTIA") Fraud Task Force ("FTF"), cellular carriers work with equipment manufacturers, service providers, and other vendors in the areas of cellular fraud prevention and detection. As part of its efforts, the FTF has implemented an extensive awareness and training program for law enforcement agencies. This program includes an overview of cellular fraud and effective investigation techniques. Classes are conducted by private investigators specializing in cellular fraud and are paid for by the CTIA.

As a result of its efforts and involvement in joint efforts such as the FTF, GTE has taken a number of steps toward preventing cellular fraud. These include:

- (1) The incorporation of pre-call validation into its cellular system to prevent "tumbling" fraud.<sup>16</sup> This feature verifies the validity of the cellular

---

<sup>16</sup> Tumbling fraud occurs when the cellular telephone's electronic serial number ("ESN") and/or mobile identification number ("MIN") is changed after each call to confuse the cellular switch, thereby allowing the call to be completed.

telephone before any charges can be incurred and has resulted in a marked decrease in tumbling fraud charges.

- (2) The creation and implementation of fraud detection and prevention software for cellular systems. GTE has made these products commercially available and they are currently being used by a number of other cellular carriers.
- (3) Meeting with representatives of other cellular carriers on a monthly basis to discuss the various methods of fraud encountered and to devise possible solutions.
- (4) Meeting with vendors of fraud prevention products on a regular basis to keep apprised of the newest technologies and innovative methods to detect and prevent fraud.

On a broader level, the cellular industry is developing two technology-based initiatives to address cellular fraud: terminal authentication and network-based fraud management systems. Terminal authentication will be a feature on digital telephones that will use private-key cryptography to validate the authenticity of the cellular telephone being used. Standards have been developed to enable terminal authentication for future cellular telephones. These standards offer considerable promise in combating fraud. For the existing cellular telephone base, network-based fraud management systems are needed to detect the existence of counterfeit cellular telephones.<sup>17</sup> Carriers need these systems to manage fraud on existing analog telephones. Both of these initiatives will continue to evolve without Commission intervention.

---

<sup>17</sup> Counterfeiting fraud occurs when an unauthorized user programs a valid subscriber ESN/MIN pair into a cellular telephone. The unauthorized user then uses the "cloned" phone, posting charges to an existing subscriber account.

The most significant problem facing cellular carriers is not the issue of liability, it is the lack of comprehensive laws designed to aid in the prevention and prosecution of the fraud that is detected. Because of the ever-changing state of technology, criminal legislation aimed at obtaining telephone service by *any* means without paying for it must be enacted. For example, as the Commission noted, "to establish access device fraud under 18 U.S.C. Section 1029 the prosecution must show that a person's account has been accessed. In many cellular fraud cases, particularly cellular tumbling, no account is accessed." (*NPRM* at ¶ 12, footnote omitted.) Loopholes such as this must be closed.

More specifically, criminal legislation should be enacted to discourage any form of tampering with cellular terminal equipment. It would thus apply to tampering with *any* authorization or security parameters within the telephone. It also should apply to the alteration of those parameters outside the telephone's internal electronics. Such legislation would be infinitely more helpful in combating fraud than the creation of an advisory committee or the mandated labeling of cellular devices. Until such prohibitions are in place, the battle against cellular fraud will be all uphill.

*In summary:* Adequate cellular fraud prevention incentives exist for cellular service providers. The numerous efforts undertaken by GTE as well as other providers underscore this fact. However, new legislation designed to specifically combat fraud is much needed to provide "bite" to this already aggressive segment of the industry.

#### **D. LINE INFORMATION DATABASE FRAUD (LIDB).**

GTE issues "joint use" calling cards<sup>18</sup> and operates its own LIDB. On intraLATA calls, GTE assumes 100 percent of the liability for losses associated with toll fraud.

---

<sup>18</sup> See *NPRM* at n.56.

GTE also assumes varying degrees of exposure in connection with interLATA traffic. Thus, GTE has a continuing and compelling interest in seeking to limit toll fraud with or without Commission involvement.

#### **1. Calling Card Fraud.**

Calling cards have become popular because they offer a more convenient way of placing a toll call.<sup>19</sup> They are now offered by all the major LECs and IXC's as well as banks and other companies. Because customers have a variety of cards to choose from, the range of card features and the associated overall level of service have become major factors in selecting a card. Thus, GTE constantly is exploring new ways in which to prevent and detect toll fraud associated with calling card use because GTE is keenly aware that a customer's experience with calling card fraud can be an extremely negative one. Consequently, the number of times such fraud occurs and the manner in which it is handled by GTE are crucial in determining whether the customer remains with GTE.<sup>20</sup> If the customer develops the impression that GTE is somehow

---

<sup>19</sup> There are substantial differences between calling card fraud and conventional credit card fraud. With conventional credit cards, the merchant validates a known amount. If the cardholder's credit limit has not been reached, the purchase is approved, unless the merchant has some other indication that the person presenting the card is not the true cardholder. The credit card issuer receives compensation in the form of a percentage of the purchase price. In contrast, with calling cards, the amount to be charged to the calling card is unknown at the time the card is presented for payment. And, for interLATA and international calls, the exchange carrier card issuer generally does not receive any portion of the IXC's revenues as compensation for use of the card.

<sup>20</sup> GTE is currently evaluating the feasibility of introducing a "Domestic-Only Calling Card" since international calling card fraud is a large part of all calling card fraud. Once introduced, this calling card would reduce the exposure of all parties for those customers that do not make international calls. However, as discussed *infra*, this type of calling card cannot be effective unless the IXC's provide the called and calling number.

negligent in preventing fraud or in handling its aftermath, that individual or company will quickly become a *former customer*.

Thus, GTE has a number of calling card fraud prevention and detection mechanisms either in place or in various stages of development and implementation. In this context, a LIDB can be an effective aid, but *only* if IXCs and AOSs access the LIDB and provide information necessary to fully utilize its inherent fraud detection capabilities.

General education is another way GTE fights calling card fraud. GTE provides valuable fraud information to its customers in a number of ways. When GTE calling cards are issued to customers, suggestions for protecting the customer's Personal Identification Number ("PIN") are included.<sup>21</sup> GTE periodically includes information with its monthly billing emphasizing the importance of customer involvement in preventing toll fraud. GTE direct mail sales literature also typically includes tips on how to prevent fraudulent use of calling cards. GTE has established an ongoing employee educational program on toll fraud aimed at employees with the most customer contact.

As a result of its efforts, GTE has become an industry leader in detecting calling card fraud. GTE has invested several million dollars to install an advanced fraud detection and calling card administration system to augment the functionality in its LIDB. Approximately two dozen GTE employees are dedicated to operating this system around-the-clock and they have achieved considerable success in limiting calling card fraud.<sup>22</sup>

GTE's system detects fraud based upon the number of call attempts, not on call duration. This system has fraud thresholds or alarms that can be set to warn operating

---

<sup>21</sup> See Attachment B

<sup>22</sup> See Attachment C. This depicts in graphical form the results of a recent study of calling card fraud associated with the use of GTE Calling Cards.

personnel of potential fraudulent calling volumes. The thresholds or alarms can be set at different levels for various call types that are likely to experience different potentials for fraud; *e.g.*, bill-to-third number, collect, domestic, and international. In the case of international calls, however, unless the IXC's provide the calling and called number along with the LIDB query, this capability cannot be used since international calls cannot be distinguished from domestic calls.<sup>23</sup>

Fraud from calls of long duration, whether placed with a calling card or not, presents a particularly difficult type of fraud to detect. In the past, this form of fraud typically was detected through *ad hoc* special studies targeting central offices with histories of high toll fraud. Several LECs have recently developed mechanized processes that examine billing records each evening and flag extremely long calls for immediate investigation. GTE piloted this type program and is currently evaluating the information gained to determine how a detection system could best be implemented in the GTE network. It is clear, however, that the system would be most effective if it was deployed by all the LECs and IXC's. This would avoid situations in which calling card fraud goes undetected because it occurs in another LEC's service territory where the LEC issuing the card is unable to monitor either the other LEC's or the IXC's network.

---

<sup>23</sup> The importance of the called and calling number in monitoring different types of calls for fraud was illustrated by a recent incident. The fraud detection system associated with the GTE LIDB alerted the attendant that a calling card issued to a large business customer was being used for a high volume of international calls. GTE was able to detect this activity because the involved IXC had provided called and calling number information along with the LIDB query. GTE immediately deactivated the card and contacted the card-holder's employer. The employer initially requested that the card be reactivated because the employee holding it was traveling on business. However, once advised that the calls in question were international, the employer immediately approved continued deactivation because such calls would be highly unusual. It was later determined that the employee was not involved in making the calls and the customer expressed appreciation for GTE's quick action in preventing a major fraud loss.

While GTE's calling card fraud detection system has already proven to be an unqualified success, its ultimate effectiveness is largely dependent upon the cooperation of both the IXC's and other LIDB owners. GTE has initiated discussions with other LIDB owners to share the knowledge gained through various operating detection systems, with the aim of learning from one another's experiences. GTE also cooperates with some IXC's regarding suspicious numbers.<sup>24</sup> Exchange carriers and IXC's also have held preliminary discussions regarding the need for a national centralized database containing suspicious numbers.<sup>25</sup> However, much work remains before it can be determined whether such a system would be viable.<sup>26</sup>

## **2. Provision of the Originating Calling Party Number and the Called Number.**

The Commission seeks comment on "whether the carriers querying LIDB should provide the LECs with the originating calling party number and the called numbers." (*NPRM* at ¶ 37.) The foregoing discussion clearly answers this question. Such information is indispensable if fraud detection systems are to reach their full level of effectiveness.

---

<sup>24</sup> Suspicious numbers may include payphones that have been used fraudulently in the past. Thus, if a LIDB threshold indicated possible fraudulent usage in progress and the called or calling number was matched to one on a suspicious number list, the investigator would be almost certain to initiate a block on the calling card involved.

<sup>25</sup> Today each LIDB owner maintains its own list of suspicious telephone numbers. Maintenance of these lists is a cumbersome, very labor-intensive process. Moreover, any given list may not include the suspicious telephone numbers located in the service territory of another LIDB owner.

<sup>26</sup> The extent to which such a system of shared information would be legally permissible must also be explored. See Section IV.B., *infra*.

Provision of this information can be accomplished either by a revision to the standards for calling card LIDB queries,<sup>27</sup> or through Commission mandate. GTE is working with IXCs to obtain this information with each LIDB query. Although all of the IXCs contacted agree that this information is beneficial, one large IXC has yet to agree to provide it.<sup>28</sup>

Moreover, exchange carriers should not be required to compensate IXCs for called and calling number information.<sup>29</sup> The cost to IXCs to upgrade their Signaling System 7 ("SS7") capability to include the called and calling number with the LIDB query is minimal, primarily involving software upgrades to existing capabilities.<sup>30</sup> And, the IXCs' reduction in losses from calling card fraud realized by the provision of this information should more than offset its relative cost in a very short period of time.

In addition, the "presence or absence of [called and calling number] information *should* affect any decision concerning the allocation of liability for toll losses." (See *NPRM* at ¶ 37, emphasis added.) If called and calling number information is not provided by IXCs, exchange carriers should not be allocated any share of liability for

---

<sup>27</sup> The American National Standards Institute ("ANSI") standard for calling card LIDB queries is T1.230-1992. This standard identifies called and calling number information as optional elements of a LIDB query message. At a recent ANSI meeting, a proposal that the ANSI standard be revised to include called and calling number information as mandatory elements received favorable response. However, full consideration and adoption of this proposal will take some time.

<sup>28</sup> Having the called and calling number not only allows a LIDB owner to establish different call volume thresholds for different types of calls, it permits calling patterns to be monitored. For example, if calls suspected of being fraudulent are occurring simultaneously from several states, the calling pattern helps confirm the presence of fraudulent activity.

<sup>29</sup> See *NPRM* at ¶ 37.

<sup>30</sup> Bellcore TR-NWT-000954, "Common Channel Signaling Network Interface Specification Supporting Alternate Billing Services" defines the necessary SS7 protocol.